Dave Aitel
Partner, Cordyceps Systems
12/6/2021

Comments on this rule may be submitted to the Federal rulemaking portal (*www.regulations.gov*). The *regulations.gov* ID for this rule is: BIS-2020-0038. Please refer to RIN 0694-AH56 in all comments.

SUMMARY:

This interim final rule outlines the progress the United States has made in export controls pertaining to cybersecurity items, revised Commerce Control List (CCL) implementation, and requests from the public information about the impact of these revised controls on U.S. industry and the cybersecurity community. Specifically, this rule establishes a new control on these items for National Security (NS) and Anti-terrorism (AT) reasons, along with a new License Exception Authorized Cybersecurity Exports (ACE) that authorizes exports of these items to most destinations except in the circumstances described. These items warrant controls because these tools could be used for surveillance, espionage, or other actions that disrupt, deny or degrade the network or devices on it.

I want to thank you in advance for reading these comments on the proposed final rule for cyber tools and the related regulatory exception (ACE). I am a specialist in information security and have been working both in the technical and policy area for over two decades. Currently I am a partner at a research and engineering firm, but none of our products and services are likely to be controlled by this regulation - in other words, I don't have a vested interest in weakening the control, but I remain familiar with it, and believe it is important and hence have a lot of thoughts.

My first and most important feedback on this control is that it is a new, highly complex control that affects a broad sweep of current and future technologies and business sectors. ACE has done a large amount of work to try to reduce secondary effects of this control, but because of that, is a tangled web of words, which can only be properly analyzed using flow charts and walking through various scenarios.

In addition, the overall context this control sits is not well understood by the community it directly affects. One question that comes up over and over in the community is around sitting at an information security conference dinner table and discussing exploitation techniques. If it's a private dinner, are people supposed to examine an ACE flowchart to figure out if they are OK to attend the dinner and have a frank discussion?

I honestly don’t know, and I’m what passes for an expert at this subject in the information security community, including, for what it’s worth, large parts of the community that directly support USG research efforts.

Many of these issues can be fixed by adding one more exception to ACE - a restriction on only having to worry about the technology controls if they are part of a commercial transaction. Tons of effort has clearly gone into ACE to avoid negatively affecting the research community, but because of a lack of clarity, we are going to force everyone in that community to hire an export control lawyer at great expense and stress - and the last thing we need is a dampening effect on our security community right now.

I think it goes unnoticed that while most export controls apply largely to companies with their own compliance departments, almost no company in this sector has any of that infrastructure. They are usually less than ten people, and spending 10K on an export control lawyer is a significant expense for them.

What we don’t have right now is any clear contact from BIS who is talking about this and can be relied upon by the community for a relationship on these issues. The NSA has Rob Joyce. CISA has Jen Easterly. Implementing controls like this is not just a ruleset you can throw over a fence - it has to be a conversation and engagement with the community. Who at BIS is that person who is going to be the point of contact? Where is the communications team pulling apart the control and ACE and doing youtube videos and answering questions on impromptu Zoom meetings? When a new person comes into the field of export control, we have to explain “specially designed” to them, and that “technology” really means “documentation”. We also have to explain what “vulnerability disclosure” means in this context. None of this can be taken for granted!

But now we have to do that to an entire economy of penetration testers and software developers. Who is responsible for doing that? Having an email address and phone number to call is not enough for something this major.

Right now, BIS is maintaining what a national security policy team would call “strategic ambiguity” with regards to how this is going to be implemented. The control is cloaked behind security through obscurity simply because it is extraordinarily complex and no effort has been made to do anything else other than drop it on the community.

In conclusion: there are scenarios where this control may have secondary effects we don’t know about yet, but getting additional clarity would not be hard - and a PR effort with the community is a good idea regardless. It would be worth delaying the final rule in order to accomplish this, if for no other reason than as a confidence building measure.